1979

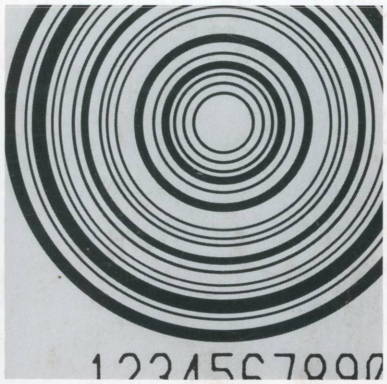
Controls over using and changing computer programs; Computer services guidelines

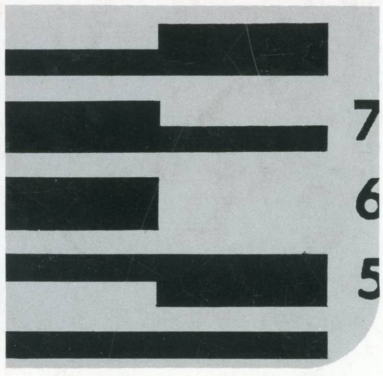
American Institute of Certified Public Accountants

COMPUTER SERVICES GUIDELINES

Controls Over Using and Changing Computer Programs

American Institute of Certified Public Accountants AICPA





Notice to Readers

This publication is issued by the American Institute of Certified Public Accountants for the information of its members and other interested parties. However, it does not represent an official position of any of the Institute's senior technical committees.

Prepared by

Program Librarian Function Task Force

Richard D. Webb, *Chairman*
Eugene A. Blish
James F. Caudle, Jr.
Alan H. Nierenberg

AICPA Staff

Carol A. Schaller, *Manager*
Computer Services

Approved by

Computer Services Executive Committee (1977–78)

Richard J. Guiltinan, *Chairman*
Lois L. Cohn
John P. Harrison
Karl G. King III
Albert A. Koch
Richard F. Maginn
John W. Nuxall
Phillip A. Parker
William E. Perry
Walter D. Pugh
Joseph D. Wesselkamper

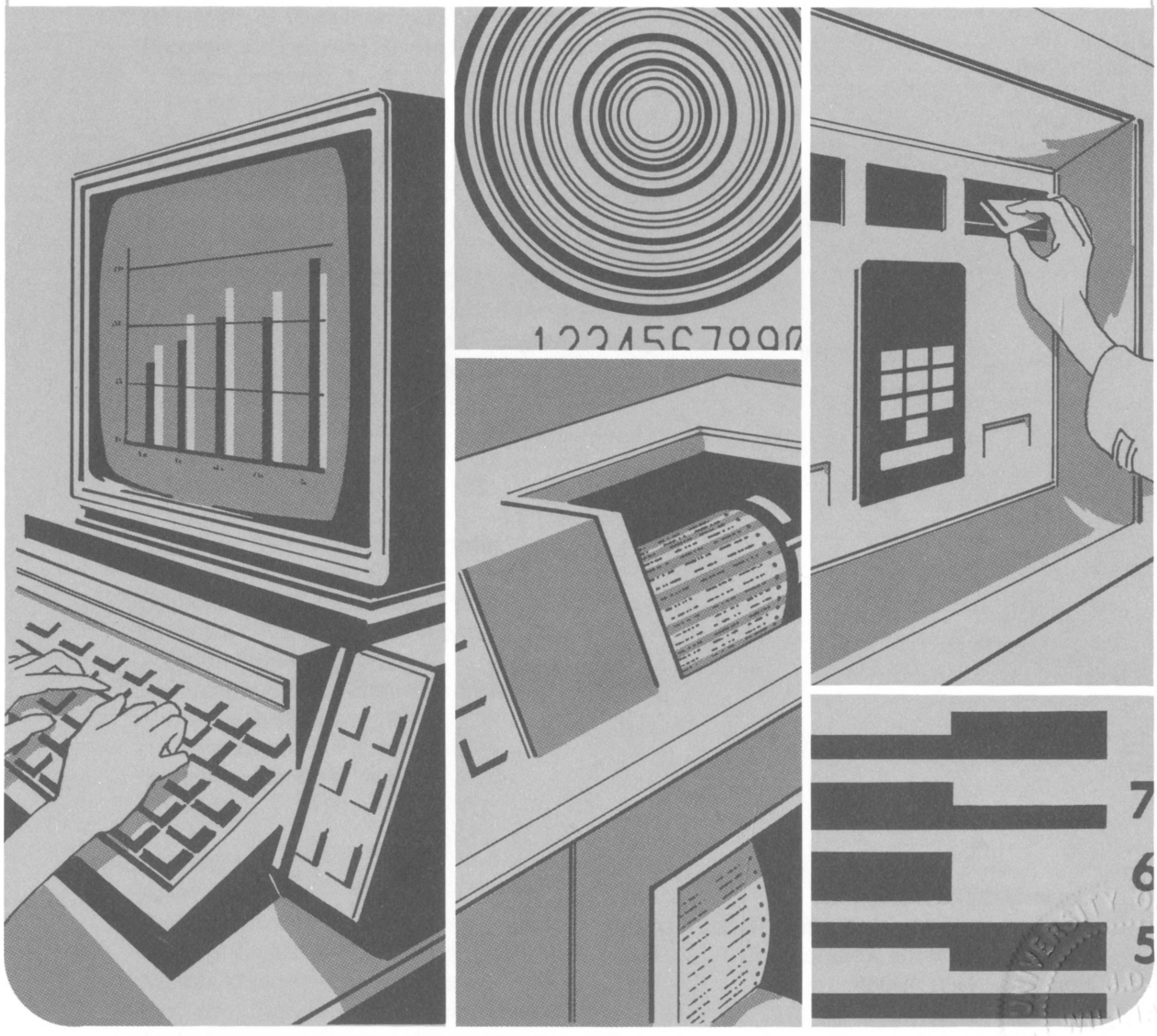
AICPA Staff

Donald L. Adams, *Vice President*
Administrative Services
Paul H. Levine, *Manager, Computer Services*

COMPUTER SERVICES GUIDELINES

Controls Over Using and Changing Computer Programs

American Institute of Certified Public Accountants AICPA



First Impression 1979

Contents

Introduction

The study of internal accounting control includes two phases:

1. Review of the system for knowledge and understanding of the procedures and methods prescribed.
2. Tests of compliance of those controls upon which reliance is planned in order to gain reasonable assurance that they are in use and are operating as planned.[1]

In a computer environment, some operations of the accounting system and some of its control procedures are performed by computer programs. Accordingly, an important part of the system of internal accounting control may be the controls over using and changing computer programs.[2]

Relevance to Management

Controls over using and changing computer programs are important to management in helping assure that transactions are processed as authorized. Controls over the *use* of programs are part of the procedures by which management authorizes the processing of transactions by computer programs. The controls over program *changes* are the procedures by which management authorizes changes to specific transaction processing and control procedures performed by the computer.

Specifically, the control objectives covered in this guideline are—

- To assure that the authorized version of the computer program is appropriately processed (controls over the use of programs).
- To assure that (1) program changes are implemented as authorized, (2) all authorized changes are made, and (3) unauthorized changes are prevented or detected (controls over program changes).

Relevance to the Auditor

This guideline deals with one aspect of the auditor's study and evaluation of internal accounting control: the auditor's consideration of whether the procedures established by management have been in use and have operated as planned throughout the period of reliance for those procedures that are performed by computer programs.[3] Specifically, this guideline discusses the auditor's understanding and evaluation of the controls intended to provide reasonable assurance that the *authorized version* of a program was *processed as authorized* throughout the period. For example, the auditor who is planning to rely on control procedures performed by a computer program (programmed controls) may wish to consider whether (1) the program containing the programmed controls to be tested for compliance is used as authorized by management so that the programmed controls are not circumvented and (2) the version of the program that the auditor plans to use in compliance testing is the version actually used in day-to-day transaction processing.

The auditor who decides to review the controls over using and changing programs should not consider only this aspect of the

1. *AICPA Professional Standards,* AU section 320.50 (New York: Commerce Clearing House).
2. This guideline may be used as an educational tool to learn about these controls or as a guide to aid in reviewing them. Readers should have a background in both EDP fundamentals and computerized accounting systems.
3. This guideline does not address how to determine whether management's authorized version of a program is proper in the circumstances. Although this is an important consideration, it is outside the scope of this document. See the AICPA audit and accounting guide, *The Auditor's Study and Evaluation of Internal Control in EDP Systems* (New York: AICPA, 1974).

system of internal accounting control. If controls are weak in these areas, the auditor should consider whether compensating controls, such as user reconciliations or balancing procedures, provide sufficient assurance that the transactions are processed correctly.

Overview

Controls over using and changing programs are relevant to entities of all sizes whether they have a large or small computer, an online or batch system, or a simple or complex system. However, the procedures used to implement the control objectives may differ, and some of the control objectives may be more difficult to accomplish in some environments. Because of the variety of company and computer sizes and sophistication, this guideline separates both the process of using programs and the process of changing programs into functional activities (for example, operating the computer or programming of changes). The control objectives for each process are discussed in terms of the responsibilities of individuals performing each activity. In this way, the auditor can assess whether the procedures performed by the person (or in some cases, programs) responsible for the activity meet the control objectives, regardless of the arrangement of the activities in the organizational structure.

Entities organize these activities in a variety of ways: sometimes by individual activity, sometimes with activities grouped in various ways, depending on whether the application is processed using batch or online techniques. Large companies frequently organize the EDP department by activity and may have several people working in each area. Small companies may have only one or two persons in the EDP department; several of the activities may be combined and authorization procedures tend to be oral or implied.

More companies of all sizes are using computers. Many companies use small "turnkey" systems that provide the computer and application software as a package. Computers installed in this manner tend to use direct or online entry of data, and the person entering the data is frequently the user. The auditor should not be misled by the apparent simplicity of a small system. Current technology permits sophisticated applications to be implemented for any size system and organization.

Some companies use service centers to process their transactions. The auditor should recognize that, under such circumstances, the control objectives and activities in using and changing programs are the same as for organizations that have an in-house computer. The difference is only in who performs the activity. The control objectives are equally important in both environments.[4]

The remaining parts of this guideline are organized as follows:

The second part discusses controls over the use of computer programs, describing—

1. The activities involved in using programs.
2. The responsibilities of each activity to help assure that the authorized version of a computer program is appropriately processed.
3. The effects of various processing environments on the controls over using programs.

The third part deals with controls over program changes, describing—

1. The activities involved in making changes to programs.
2. The responsibilities of each activity to help assure that program changes are implemented as authorized, that all authorized changes are made, and that unauthorized changes are prevented or detected.
3. The effects of various processing environments on the controls over program changes.

Last is a case study illustrating an auditor's study and evaluation of controls over using and changing computer programs.

4. See the AICPA audit guide, *Audits of Service-Center-Produced Records* (New York: AICPA, 1974).

Controls Over the Use of Computer Programs

A broad objective of control over computer programs is to ensure that the programs are processed as authorized by management. The issues are Who has access to the programs and how are they used?

Processing Activities

Automated accounting systems normally include the following activities:

- Initiation of transactions[1]
- Conversion of transactions into machine-readable form
- Storage of data files and programs
- Computer processing of transactions
- Output distribution

This section discusses objectives of control over the use of programs within each of these activities, as well as—

- Procedures for detection of unauthorized use of programs.
- Control considerations in various program processing environments, including batch systems, library software, online systems, minicomputers, and service centers.

In evaluating its system of internal accounting control, management should consider whether the person(s) or program(s) performing the activities fulfill the responsibilities for control discussed below. The auditor should consider these client responsibilities for control in the study and evaluation of internal accounting control to determine the scope of substantive audit procedures.

Initiation of Transactions. Initiation of transactions normally takes place in the user department (for example, the order entry or payroll department). User department personnel approve transactions and send them to the EDP department with their authorization to process the transactions using the approved computer program.[2] The authorization could be documented, oral, or implied by such action as delivery of the document or online entry of the transaction.

The user department is responsible for many control procedures that do not involve the use of computer programs (for example, manual processing of all transactions according to established policies and procedures before sending them to the EDP department). These procedures are not discussed in this guideline. The following are the user's responsibilities for authorizing the use of programs:

- Approving accepted transactions for processing by the application program.
- Establishing and maintaining documentation of processing authorization.

Conversion of Transactions Into Machine-Readable Form. This activity usually takes place within the EDP department and generally consists of keying information contained on transaction source documents onto cards, tape, disk, or other magnetic media, or direct online file update via a computer terminal. Some companies may perform some or all of the data conversion within the user department. Within this activity, the responsibilities for control over using programs include—

- Accepting only transactions that are approved for processing.

1. As used in this guideline the term *transaction* includes all transaction types defined for an application. For example, a transaction could be a file maintenance, update, or error correction transaction. Computer-generated transactions are not discussed under this activity because they are a result of processing the programs. Their initiation is controlled by controlling the processing of the program and program design.

2. This starts the process of authorizing use of a program.

- Establishing and maintaining documentation of approval of further processing.

Storage of Data Files and Programs. This activity generally is located within the EDP department and consists of one or more areas called *libraries* to which access is limited to authorized individuals. A library is used for storing data files, programs, and, in some cases, documentation. Certain data files and programs may be available on the computer continuously (online). Whether the data is in a physically separate area or online, the responsibilities within this activity include—

- Releasing approved programs, data files, or documentation to authorized personnel based on approved requests.
- Establishing and maintaining documentation of authorized release and return of programs, data files, and documentation.
- Accounting periodically for all programs, data files, and documentation.

Computer Processing of Transactions. Although this activity normally is performed within a central EDP department, occasionally it is done in user departments. In general, this activity receives data, processes it using approved programs, and returns the output. Regardless of the organizational location of this activity, the responsibilities for control over the use of programs include—

- Accepting only approved requests for processing.
- Processing the transactions according to approved procedures.
- Distributing the results of processing as authorized.
- Establishing and maintaining documentation of completion and release of processing.

Output Distribution. This activity usually is performed by the user department, EDP personnel, or an EDP control group. Responsibilities within this activity include—

- Reviewing processed transactions and other output to determine whether they were processed as authorized.
- Distributing the output as authorized.
- Establishing and maintaining documentation of release of the output as authorized.

Detection of Unauthorized Use of Programs

When the controls do not operate as anticipated or may have been circumvented, management should consider reviewing the console log or job accounting data periodically. This information generally contains the names of programs or jobs processed, time of day and duration of processing, system error conditions, and operator interventions. This review could alert management to unauthorized use or could identify use of software that could change programs. The information, however, may not reflect use of programs outside the controls provided by the operating system.

Program Processing Environments

The foregoing activities occur under differing organizational structures using many different data processing techniques. The following sections clarify how the control responsibilities for each activity can be met in various processing environments, including—

- Batch systems (including the effects of an operating system)
- Program library software systems
- Online systems
- Minicomputers
- Service centers

Batch Systems. To simplify the explanation of how an entity could organize the activities and fulfill the control responsibilities, examples are presented to illustrate possible control procedures. The initial example illustrates the processing activities and their respective control responsibilities in a batch environment. The initial example is followed by considerations in more complex systems and by examples of the effects of the data processing environment on control over the use of programs.

This example is an order processing system in an organization in which the user department is solely responsible for the initiation activity, and the EDP facility is organized into four departments, as follows: data control, data entry, library, and computer operations.

1. Telephone and mail orders are received in the order entry (user) department, where they are approved. The following procedures are then performed:
   a. Periodically throughout the day, approved orders are grouped into batches and a control document ("transmittal" form) is prepared, reviewed, and approved.
   b. Approved batches are noted in a batch control log and sent to the EDP facility.
2. The data control department receives the batch:
   a. Reviews the transmittal for proper authorization and notes the arrival in a log.
   b. Sends the batch to data entry for conversion and notes it in a log.
3. The data entry department receives the batch:
   a. Reviews the transmittal for proper authorization.
   b. Transcribes the data according to approved procedures and cancels the source documents.
   c. Returns the batch (source documents and converted data, such as cards, tapes, diskettes) to the data control department.
4. The data control department receives the cancelled source documents and the converted data:
   a. Prepares a "run request" form designating the program/procedure and data files to be processed.
   b. Sends the batch (converted data and run request) to the computer operations department, noting it in a log.
5. The computer operations department receives the batch:
   a. Reviews the run request for proper approval and notes the run request in a log.
   b. Uses the run request as authorization to obtain the data file(s), program(s), and operation(s) documentation from the library.
6. The librarian receives the run request:
   a. Examines the run request for proper approval.
   b. Selects the requested items.
   c. Notes release of requested items in a log.
   d. Turns the requested item(s) over to operations.
7. The operator receives the items necessary for processing:
   a. Loads the program into the computer and mounts the files as prescribed.
   b. Processes the items:
      (1) Returns programs, files, transactions, and documentation to the librarian.
      (2) Sends the output reports and run request to the data control department after noting it in a log.
8. The data control department receives the items from operations:
   a. Reviews the items to ascertain that only authorized processing was performed.
   b. Notes all accepted items in a log and approves the run request as complete.
   c. Returns the output and cancelled source documents with a signed transmittal to the user department, noting it in a log.
9. The user department receives items from the data control department, reviews the items for authorized processing, and notes accepted batches in a log.

Although almost all computers have operating systems, the foregoing example does not describe operating system considerations in order to highlight manual procedures that might be used. However, operating systems are significant in control over the use of programs.

Operating System Considerations. The operating system performs some of the procedures involved in using programs, such as maintaining programs in an online disk file library and printing a console log of operator instructions and actions. Operating systems also facilitate file label checking, which helps to assure that the mounted file is the one requested by the program. Although this is not a direct authorization control, it is a detective control to help assure that the librarian issues, and the operator mounts, the proper file.

The ability to store programs on a disk file ready to be executed is one advantage of using operating system software. The computer operations department need only enter a command through the console or other input device to initiate and process the desired program. This feature relieves the librarian from responsibilities related to releasing programs and consolidates the transaction processing flow into one

authorization step. This results in concentrating more responsibility in the EDP operations department. Operating systems may also automate portions of the program library addition, change, and deletion procedures. Controls over these procedures are discussed in the next chapter.

The example discussed above may change as follows when an operating system is employed:

1. The data control department (or a scheduling group that is part of the control department), in addition to the run request, may prepare operating system control statements to process the program. These statements include, among other things, an identification of the job to be processed, the name of the program to be processed, and, when required by the operating system, names of files to be mounted. Occasionally, special operator instructions are included.
2. The EDP operations department uses the run request as authorization to obtain data files from the library and mounts them according to instructions generated by the operating system and printed on the operator's console or in a "run book." This latter approach combines activities in the operations department. Generally, this lack of segregation of functions is compensated for by strong supervisory controls, limitation of access to the computer by other than operations personnel, and other controls to assure the authorized program was processed at the proper time with the proper files.

   Another possible control procedure involves the activity log that most operating systems produce. The log may be reviewed and approved by management, usually by an operations supervisor. After processing, the operations department returns all items to the data control department. A copy of the console log may also be included.
3. The data control department personnel perform procedures as before. The primary difference may be the addition of a review of the console log to determine whether processing was performed as authorized.

Some organizations use an approach different from that described in the foregoing examples. They focus most EDP department activity in the data control department, including the data file library. Under these circumstances, the data control department obtains the appropriate data file(s) and includes it with the package sent to the EDP operations department. When this is done, the operator gets everything necessary to process the program directly from the data control department. Although this concentrates more control in the data control department, the responsibilities are generally compatible. If several people work in the data control department, the library may still function separately, but it will deal with other control personnel rather than operations personnel.

Program Library Software Systems. In addition to operating system software, the auditor often encounters other software the company has developed or purchased to make operations more effective and efficient.

Various library software systems can be used to support objectives of control over the use of computer programs. Some of the library software that has been developed is included in the operating system and some are separate systems. Common capabilities of the software are these:

- Maintaining an inventory of the files stored in the library.[3] This does not, however, eliminate the librarian's responsibility to release data files only to authorized persons based on approved requests.
- Storing control statements for processing programs or a series of programs.
- Storing executable programs.
- Storing documentation, including operator instructions for various programs.
- Maintaining a directory of all current production source programs. (Note: source programs may be changed frequently, as is discussed in "Controls Over Program Changes").
- Keeping track of disk files that are continuously mounted online. Many files may be kept on a single disk, and operating system software is generally used to keep track of their location and status.

Online Systems. Technological advances in hardware and software have allowed more of the program authorization structure to be automated. Terminals have placed the users in direct contact with the computer. Although the organizational structure may be different in an online system, the auditor's concern about control is not. The activities may be automated, but individual control responsibilities within those activities still exist.

3. The files could include data, programs, and documentation.

The auditor may encounter one or more of the following situations in the user department:

- One or more terminals may be connected to the computer. Processing of transactions may range from data entry to online update or inquiry of master files.
- One or more "intelligent" terminals may be used. In addition to being connected to the computer as described above, some programs are processed *within the terminals* to minimize transmission costs and processing demands at the central location (for example, password authorization or transaction editing).
- One or more terminals may be connected to one or more minicomputers that are connected to a central computer. This configuration is used when certain processing is unique to the user department, and files and programs are most appropriately kept within the control of the user department. This configuration also permits a certain amount of "preprocessing" of transactions that can limit the volume of transmitted data and processing demands on the central computer.

The following example illustrates how management might control the use of computer programs when the user communicates with the computer via a simple terminal. The discussion focuses on authorization of the use of programs and does not discuss the other control objectives the auditor should consider.

In this example, orders are received by mail or phone, and a customer order form is completed. This might be done in several ways:

1. The order information is entered manually on a form, is reviewed, approved, and given to the terminal operator for entry into the system. The orders could be entered separately or in batches.
2. The order information is typed on the form displayed by the terminal, so data entry and order form completion take place simultaneously.
3. The order information is entered via the terminal, and order forms are periodically printed at the central computer site and sent to the order department.

The primary distinction between an online system and a batch processing system is the reduction of human involvement. This does not necessarily mean fewer personnel in the EDP facility, but it does mean realignment of their responsibilities. Illustrations of how control objectives can be implemented in an online environment follow.

Possible Controls Within the User Department. Changes in the organizational structure may be merely the addition of a terminal operator, or existing personnel within the user department may be trained to operate the terminal. General authority of department personnel to write orders does not usually change, and persons specifically authorized to use the terminal should be designated. This results in a control to limit physical access to the terminal to authorized persons.

Other possible authorization control procedures within the user department include—

- Requiring the operator to use a key to activate the terminal.
- Using a security device that requires insertion of a card with identifying information.
- Using a hardware identification facility within the terminal.
- Requiring the operator to enter unique or confidential information to establish identity to the computer, such as the operator's name or initials or a password.

Software can be used to check one or more of these procedures to establish that the combination is valid and the operator has the proper authority. Whenever passwords are used, management should consider monitoring to detect improper use of the passwords. One way this may be accomplished is by designing and writing a special program to print all invalid attempts to access a production program. All information captured by the system pertaining to the invalid attempt should be printed on a report and analyzed by a proper authority to identify and trace unauthorized attempts. Depending on the sensitivity of the application, other more elaborate procedures may be employed to raise the level of assurance that the person at the terminal has the appropriate authority.

Once the operator is identified as authorized to use the terminal, the system should determine if the nature of the work requested is within the operator's authority. Accordingly, the operator may enter one or more of the following:

- Name of the program to be executed.
- Name of the file(s) to be accessed.
- Type of transaction to be entered.

Software can be used to verify the request and authorize continuation of processing. The operator could then start processing the request.

In summary, these procedures may provide reasonable assurance that the processing of transactions, and access to and use of programs, are authorized by programmed criteria that were approved by management when the system was installed.

Possible Controls Within the EDP Department. An online environment may significantly change the control procedures over use of a given application program. The control procedures in an online EDP facility are largely embodied in software. Manual control procedures are reduced because only offline files are handled manually. Offline file requests are usually infrequent, because required data files are continuously available on the system.

The reduction of the human element makes automating control procedures a complex task. Computer identification of a user differs from human identification of a user. Accordingly, development, maintenance, and review of identification software are important because the effects of the authority embedded in software are often pervasive in a business entity. The procedures that control the use of programs may be more complex in online systems than manual or batch systems, but the activities and control responsibilities remain the same.

Minicomputers. Current technology makes it economically feasible to perform all functions of an EDP facility in the user department. Even though the activities are performed by the users, the responsibilities for control pertaining to processing activities should be considered. Additional considerations include these:

- The level of control provided by segregation of functions is often significantly reduced.
- Many minicomputer applications operate online, and the considerations and techniques for online systems may be applicable.

Service Centers. When a service center is used to process financial data, some of the processing activities are performed by the service center rather than company personnel. The responsibilities pertaining to processing activities should still be met, or compensating controls such as user reconciliations should be developed to achieve the control objectives. The auditor may visit the service center or use a third-party auditor's report to learn whether the control responsibilities are being met by the service center. Third-party reviews are discussed in the AICPA audit guide, *Audits of Service-Center-Produced Records.*

Conclusion

Achieving objectives of control over the use of programs should help prevent or detect errors or irregularities, such as programs processed—

- By an unauthorized user.
- At an unauthorized time or date.
- With the wrong or unauthorized data.
- In place of the proper program (for example, the wrong program in a sequence of programs in an application system).

Controls Over Program Changes

This section discusses controls related to assuring (1) that changes made in current production programs were authorized and (2) that all authorized changes were made and implemented properly, so that current production programs remain authorized.[1]

The section discusses—

- Effects of changes in production programs.
- Significance of controls over program changes.
- Common ways that managements implement the program change process.
- Activities in the program change process and the control responsibilities within each activity.
- Program change considerations in various EDP operating environments, including batch systems, library software, online systems, minicomputers, and service centers.

Effects of Changes in Production Programs

Production programs are designed to embody accounting and control procedures. Programs should reflect only the procedures established by management.[2] Whether a processing system is manual or computerized, unauthorized changes or errors made in changing procedures can cause disruption and slow detection of errors, if errors are detected at all.

In computerized systems, the impact of a change can be especially subtle and pervasive because the procedures are "invisible." People, who would tend to notice if something were unreasonable, are not involved in many of the procedures. In data base environments, there may be many users of the same data, so an error can have wide-ranging effects. For example, an insurance company made a simple modification to part of a data base application, changing the mode of payout for life insurance claims. Because the change was not properly tested, an error occurred in a portion of the data base used by another application. The effects showed up in a seemingly unrelated part of the data base, causing life insurance agents' commissions to be overpaid.

Significance of Controls Over Program Changes

A program becomes a production program after a number of tests and approvals indicate that it reflects management's authorized procedures. Management then depends upon controls over program changes to assure that the program remains the authorized version. Although management should direct a major effort towards *preventing* unauthorized or accidental access to production programs (for example, segregation of functions and the effective use of passwords), it should also develop procedures to *detect* and *monitor* access to programs for change purposes.

Most computers have utility software that, among other things, can be used to circumvent certain controls to resolve a software problem quickly. Some of these utility programs can be processed without leaving

1. The objectives of controls over changes to production programs also apply to operating systems, system software (utilities, communications), and backup and recovery programs.

2. Although the program change process is similar to system development, the procedures for developing new programs are not within the scope of this guideline.

evidence of their use. Accordingly, they are a potential threat to the overall system of internal accounting control. Such software is helpful in emergency conditions, but a well-designed system should not require its use except in rare circumstances. When it is used, management should supervise its processing and follow up the impact on production processing.

When the auditor judges that it is appropriate to review a production program (for example, by reviewing documentation or program code or using test data), the review is only performed at specific times during the audit period. The controls over program changes should provide reasonable assurance that the program is the same (or modified in an authorized manner) during the intervening times. The auditor may find it helpful to rely on controls over program changes for two reasons:

1. If the auditor determines that the program change controls are sufficient and working, the auditor could rely on the program to be either the same as it was at the time of the initial review or modified with known authorized changes. The auditor would then review the changes (rather than the entire program) to determine their effects on the planned audit approach.

2. When planning to rely on control procedures performed by a program (programmed controls), the auditor should consider how the program being compliance tested relates to the version actually used for processing throughout the period of reliance. Determining the relationship of the versions is facilitated if the auditor can rely on the controls over program changes.

Common Ways That Managements Implement the Program Change Process

The following are some examples of implementations of the production program change process:

- Management physically secures the production copies of the programs. A duplicate copy is prepared for modification and test purposes. The programmers are allowed to use the test copies, but not the copies used for production. The programs can be located in separate libraries, or can be in the same library, distinguished by "test" or "production" identifications. When the programmer has completed a change and it has been appropriately tested and approved, the approved copy replaces the old production copy.
- Some entities that use vendor-supplied software keep the original source code program intact and maintain a separate source code for changes. When a change is made, the original source code is recompiled with the changes and both are physically secured.
- Program library software may be used, as is discussed in detail in this chapter.

Program Change Activities

Managements handle program changes in different ways, but the activities normally are—

- Requesting
- Designing
- Programming
- Testing
- Implementing

Companies with few EDP personnel tend to be organized informally and to rely on management supervision to assure that activities are working as desired. Other companies may be highly structured, with the various activities assigned to specialized personnel or to project teams responsible for implementing changes. Some companies also

use an EDP steering committee of high-level personnel from areas in the organization affected by EDP. Their role is usually overall guidance, but that role may include approval of certain major system changes. Some companies that have internal auditors may involve them in program changes.[3] Their role often consists of reviewing a change before it is implemented for the anticipated effect on company policies, operations, or controls. Auditors may also be involved throughout the program change process.

The structure of the EDP department is less important than the attainment of the specific control objectives. The following paragraphs discuss the control objectives for each of the program change activities.

Requesting the Change. A computer application is developed to meet the needs of some function in an organization (for example, order entry or billing). Although the user department generally performs manual control procedures rather than EDP controls, the user's role is essential in achieving overall accounting control objectives. In general, the user's role in making changes to application programs may be described as a check and balance function against the data processing department. The program change cycle normally begins with a user-initiated change request and ends with the user authorizing the data processing department to implement the change.

The responsibilities for control over program changes to be met by the user department are—

- Initiating requests within the scope of its authority, as delegated by management.
- Documenting the requests and subsequent approvals.
- Approving changes before they are implemented, based on review of changes to affected manual procedures and associated training.
- Approving changes before they are implemented, based on results of appropriate testing procedures.

Program changes may be requested by departments other than the users (for example, the computer operations section may request a change to improve operational efficiency of the system, or the internal auditors may request a change to improve control procedures). Hardware and software vendors may also initiate modifications. Before any change is implemented, the users responsible for the application should obtain assurance that the change does not adversely affect their use of the system. Users should do this by testing the application regardless of where the change originated.

Designing the Change. The design activity generally is performed by the systems and programming section of the EDP department, although, in large organizations, it may be performed by the user department. Usually the systems analyst works with the user to define the specific technical changes required (for example, a change in the design of a report, formula, calculation, or input document). When the design is complete and documented, both the user and systems and programming management approve the change before programming begins.

The responsibilities for control over program changes to be met by individuals involved in the design activity are—

- Accepting only authorized requests for program changes.
- Designing changes within the bounds of established design and documentation standards.
- Obtaining user approval for the design.
- Providing the change specifications to the programmer and authorizing release of the existing documentation and source version of the program necessary to make the change.
- Preparing or updating appropriate documentation to reflect the change accurately.
- Reviewing changed program documentation and tests and approving them before requesting approval from the user.
- Obtaining approval from the user to implement the changed program.

If the design activity is within the user department, the auditor should consider the organizational structure of the department with respect to segregation of functions.

Programming the Change. The programming activity is usually performed within the systems and programming section of the EDP department. Sometimes programming may be done by members of the user department, and sometimes the

3. In some cases, the external auditor and consultants may be involved.

programmer and the analyst are the same person. Normally, the programmer begins with the documentation provided by the analyst. Although the change should be based on that documentation, continual discussion with the analyst is often necessary.

The programming of changes involves adding, revising, and deleting source statements in a program or operating system control statements. Sometimes this involves adding or deleting entire programs in an application system.

Programmers, regardless of their location in the entity's organizational structure, have the following responsibilities for control over program changes:

- Accepting only authorized change instructions.
- Making only the changes requested and within established programming policies and standards.
- Testing the changed program thoroughly before submitting it to the design activity for approval.
- Preparing or updating the appropriate documentation to reflect the change accurately.

Testing the Changed Program. To help assure that a change in one program does not have an unintended effect on another program or file within the system, the originating department, a quality assurance group, or some other appropriate department should perform independent tests of the program or programs before implementation. The department(s) or group that performs the testing has the following control responsibilities:

- Designing tests that exercise the program as it will be used in a production mode.
- Preparing test data that (1) simulate the normal processing, (2) test error conditions and unusual situations, such as exception transactions, maximum file sizes, transaction volumes, and other technical considerations, and (3) test the impact on other related programs or files.
- Performing the tests with extracts from "live" files or with the test data.
- Reviewing and approving tests performed by other activities, as appropriate.

Implementing the Change. The last activity in the program change process is to transfer the revised program to production status. In many systems, this consists of designating the new tested version of the program as a production program. In some systems, this may be as simple as renaming the new version and deleting the old. More commonly, it will involve copying the new version into a separate "production library."

This activity is normally performed by the operations section on authorization from systems and programming management. The responsibilities for control over program changes involved in this activity are—

- Implementing only those programs that have been properly authorized by systems and programming management.
- Accepting only those programs where the impact of the change on the operations section is known and agreed upon.

The responsibilities discussed for program change activities are applicable to both large and small companies. The method of implementation, however, may differ depending on company size and organizational structure.

Detection of Unauthorized Program Changes

The controls previously discussed in this section are essentially preventive. Management should also include controls to detect unauthorized or inadvertent changes to programs. One technique management could use is to compare the source or object code with a control copy from time to time to detect changes. This comparison could be done manually or by a computer program. Use of software for program comparison is discussed in the AICPA audit and accounting guide, *Computer Assisted Audit Techniques.* Identified changes may subsequently be reviewed to see if they were authorized. Also, some companies use a hash total technique whereby the values of each character (word, position, byte) of a program are added together. The total is retained as a control

value, and, periodically, the program code is totaled and compared to the control value. When a difference is identified, management should determine the nature of the change.

Program Change Environments

The following paragraphs discuss the impact of various data processing environments on the control objectives:

- Batch systems (including the effects of an operating system)
- Program library software
- Online systems
- Minicomputers
- Service centers

Batch Systems. In a batch system, many of the program change procedures may be implemented manually (although it is possible to enter changes online). The programmer adds, deletes, and changes source statements and then recompiles the program. An illustration of one possible program change process in a batch environment follows.

In this example, the user department is the order entry department, and the EDP facility includes data control, data entry, program library, computer operations, and systems and programming departments. The program change is to add the projected shipping date to the open order status report. One series of procedures for making the change might be as follows:

1. The user department personnel answer inquiries from customers about the expected shipping dates. They wish to add "projected shipping date" to the status report so that most customers' inquiries could be answered more quickly and efficiently. A written request for the change is prepared and sent to the systems and programming department.
2. The systems and programming department receives the request, logs it, and gives it to an analyst to determine feasibility and cost.
3. The analyst meets with the user department supervisor to determine the specific requirements, such as whether there is space on the status report for the date and how and where the date can be obtained.
4. The analyst identifies the specific technical changes necessary in the report program and data file. The analyst prepares a revised report and record layout forms, designs an input document, and prepares flowcharts reflecting the changes.
5. The analyst's supervisor reviews the design and arranges a meeting with the user to agree upon the final specifications. This is evidenced by initialling a project control sheet.
6. The analyst discusses the change with the programmer assigned and gives the programmer the documentation prepared for the change and a list of other documentation the programmer will require, such as the program name and source code listings.
7. The programmer, using the approved project control sheet as authority, goes to the program library to obtain the necessary documentation and a test copy of the source code.
8. The programmer codes the change, noting it on the latest source listing. It is submitted to data entry for keying. (The installation uses punched cards.)
9. After keying, the programmer inserts the cards into the source deck and submits it to the operations department for compilation. Operations handles the program compilation as though it were processing an application program and the source cards were transactions. After completion, operations returns the source deck and source listing to the programmer.
10. The programmer reviews the results of the compilation and, if necessary, submits additional changes or corrections until the compilation contains no syntax errors.
11. The programmer prepares test data and/or prepares test files to determine whether the program works as expected. The tests are submitted to operations on the same basis as processing an application program within the established processing control structure.
12. Once the programmer is satisfied that the changes have been made completely and correctly, the program is submitted to the analyst for approval. The analyst reviews

the changes and may also process test data.

13. After the analyst reviews it, the user is asked to approve the change. The user reviews the output and processes test data. Once the user is satisfied that the application is functioning as expected, the user signs the project control sheet, and the systems and programming department uses that approval to direct operations to start using the new version of the program for production.
14. The operations department, based on the approved project control sheet, places the new object code in the production program library and uses it until further notice.

Operating Systems Considerations. Operating systems provide many library control procedures. One capability of an operating system permits direct replacement of executable programs in the production program library. The operations department usually requires special procedures (within the standard production processing structure) to replace production programs. The program that performs the replacement function usually provides limited documentation of its processing; therefore, close supervision is generally required.

Program Library Software Systems. In addition to the operating system software, the auditor will often encounter other programs the company has developed or purchased to assist in making program changes. The most common software can be classified as "source program library maintenance software" and "executable program library maintenance software." Both are available from hardware and software vendors. The software can operate in both batch and online environments; the previous discussion of control over the use of programs also applies to this software. Some program library software provides the option to install comprehensive techniques for control over program changes, but other library software merely automates certain program change functions. Even when optional control facilities are provided, the company may choose not to implement these options. Therefore, when appropriate, the auditor should identify the library software used by the company and understand the control facilities available and the options implemented to meet control objectives.

Source program library maintenance software assists the programmer in making program changes and storing source code on magnetic files such as tapes or disks. It may also provide for increased control over access to and changes in program source code, as well as more effective review and supervision of the programmer. As is done with manual procedures, the auditor should assess the impact on controls.

Source library maintenance software reduces the amount of program handling, thus reducing the probability of lost, resequenced, or duplicated program code. Generally, the programmer need only submit statements for the code to be changed and the software makes the changes and prepares the source statements for compilation. The revised program is then compiled and the resulting executable code is stored in the library. The programmer may receive the statements that were submitted and a report of the changes that were made. Available software may offer many features to aid the programmer, but the following discussion is limited to the features that most affect the auditor's understanding of the control aspects of the software.

Processing performed by the library software is based on control statements that add, delete, or change the program source statements stored on tape or disk files. Input of the control statements can be in batch mode or online. Output generally consists of revised source statements on the magnetic media, operating system control statements to compile the revised code, reports showing changes in the specific program, and, if requested, a variety of reports showing the current status of all programs on the file.

Controls Over the Use of Library Software. Library maintenance software usually has many features. Companies that use this software should use its facilities to prevent and detect unauthorized program changes and should carefully control use of the library software capabilities. That is, a programmer's use of the library maintenance software should be limited to only those features that are needed to make the changes the programmer is authorized to make. Other features should be used by management to review and control programmers' changes.

Management's control objectives can generally be met if library software commands permitted for programmers' use are limited to those needed to change specific statements in specific programs. Examples of the software facilities that may be appropriate for programmers' use are these:

- Changing only programs with "test" status.
- Copying programs with "test" status.

- Adding programs with "test" status to the library.
- Inserting, adding, moving, or replacing one or more source statements.
- Adding or inserting comments about a change.

Various authorization schemes, such as passwords, can be used to restrict use of library software functions, and some packages permit encryption of the source statements, including a provision for an encrypt/decrypt key for each program.

Management should review the work of programmers. Library maintenance software provides facilities to assist management in carrying out this responsibility. Management can—

- Review reports that show what the programmer changed and how.
- Limit the programmer's access to programs or portions of programs, through supervision or software controls, to those necessary to carry out authorized duties.
- Supervise directly all changes of programs to "production" status when revised programs have been approved by appropriate parties.

Examples of reports that the library software may prepare for management's review include these:

1. A listing of programs (see example 1) showing
   - Date and time of run.
   - Program identification.
   - Program description.
   - Date created.
   - Date last copied.
   - Date last changed.
2. A summary of changes (see example 2) showing
   - Date and time of the run.
   - Identification of program changed.
   - Programmer who made the change.
   - Commentary, if any.
   - List of commands used and the results (for example, a command to delete a source statement is listed, followed by the actual statement deleted).
3. Source code listing with the dates created or last changed for each statement.

The software may also provide a report on all programs assigned to a programmer, listing the programs by name and current status, and a report on the status of all programs with their activity dates. Management review of these reports can provide a valuable control.

Information Maintained by Library Software. Both management and the auditor may find it useful to be aware of the types of information maintained by library software. In understanding control procedures and designing potential compliance tests, the auditor should consider what information is maintained by the program library software; usually source statements for each program are stored on a master file with a header or control record for each program. The master file is the primary file used by all programs in the system, and some library software provides for creation and maintenance of backup files.

The library software control record normally includes, among other things, the following information about a program:

- Program name.
- Version or level identification (in some systems, both).
- Program language.
- Identification code.
- Status (test or production).
- Various dates (such as creation date and date of last activity).
- Type of last activity.
- Number of source statements.

Available software may or may not include a specific control record, but the system should be able to provide the following information or its equivalent.

Program name. Program name is used by the software to locate the program to be changed. Normally, companies develop meaningful program naming conventions so that programs have names that correspond to the functions of the programs.

Version or level identification. Each time a program is changed, a sequential number or date and time is inserted automatically by the software. The next modification may use the version identification for control purposes. The number may be only in the control record or in each source statement as part of the statement sequence number. The auditor may wish to use the version or level identification to determine whether any changes have been made since the last review. If the identification is indicated in each source statement sequence number, the auditor would be able to locate and review those statements that had changed since the previous review.

Program language. The source language may be identified so that the software can

EXAMPLE 1

SOURCE LIBRARY STATUS REPORT

DATE: 02/20/XX TIME: 1523

PROGRAM IDENT	PROGRAM DESCRIPTION	CREATION DATE	DATE LAST COPIED	DATE LAST CHANGED
PAY01	PAYROLL EDIT	01/24/XX	12/04/XX	12/31/XX
PAY03	UPDATE PAYROLL MAST	12/12/XX	11/08/XX	NONE
PAY09	PRINT PAY CHECKS	09/27/XX	07/07/XX	11/07/XX

EXAMPLE 2

SUMMARY OF PROGRAM CHANGES

DATE: 08/20/XX TIME: 0937

PROGRAM-ID: PAY01

PROGRAM DESCRIPTION: PAYROLL EDIT

DATE CREATED: 01/24/XX

PROGRAMMER: FELIPE

LINE NO.	CHANGES FROM:	TO:	COMMENTS:
031001	MOVE WS-END-TEXT TO M1-MID-TEXT	MOVE WS-END-TEXT TO M1-END-TEXT	CHANGE
031300		MOVE SPACES TO RA-TEXT	ADDITION
031600	CLOSE PRODUCT-MASTER-FILE LOCK	CLOSE PRODUCT-MASTER-FILE RELEASE	CHANGE
032000	MOVE SPACE TO RA-HOME		DELETION
032180	IF NEXT-CNT NOT = 2	IF NEXT-CNT NOT = 12	CHANGE

perform certain optional edit checks on the source statements to minimize syntax errors during compilation.

Identification code. An identification code, such as a number or initials, may be included to identify the programmer. It may also be used to control access to programs and to identify who is authorized to make various types of program changes. The auditor may use this information when considering segregation of functions.

Status. The status of each program is normally included in the control record to indicate whether the program is a "production" or a "test" version. Management should not permit programs identified as "production" to be changed by programmers.

Various dates. Generally, dates are stored in the control record to indicate when the program was added to the file, or when it was last copied or last changed.

Type of last activity. The control record will often indicate the nature of the last change activity, such as "added," "changed," "copied," or "deleted." Deletion should automatically involve creation of a backup copy before physical removal from the production library. Some systems have a facility to allow retrieval of any past version of an updated program, even though old versions are removed from the active library.

Number of source statements. Counts of source statements are generally maintained and can be used as control totals together with manual control procedures.

Other Library Software Features. The following features of the source library maintenance software are also of interest to the auditor:

- The auditor can use the library software facilities to scan the program library and print a list of all occurrences of a particular data name or element. This facility can aid the auditor in locating a specific occurrence of a change. For example, the auditor might want to scan all programs for a particularly sensitive data element, such as pay rate.
- Based on an analysis of the program library, a cross-reference listing can be produced for all programs that use other programs, common modules, or subroutines. It lists all intra-library references in both directions. The auditor may use this feature to understand interrelationships of various programs and to identify potentially unauthorized modules.
- Some library software provides for the automatic creation and maintenance of backup files.

This section has discussed software for maintenance of *source* statement libraries. Although this is an important aspect of control over program changes, it is still necessary to compile the production source version of the program and replace the executable code in the executable library to have an operational production program. Software is available to control executable libraries in much the same manner as source library software. It provides several levels of security over who can use specific commands and programs in the executable library. Information about program executions may also be provided for reporting and management review purposes.

Control over program changes should include both the source and executable program libraries. A computer prepared report could be developed to provide a cross-reference between the corresponding source and executable program versions. Management analysis of such a report could identify programs that should be investigated. For example, all executable programs should have a corresponding source version.

Online Systems. The differences between an online environment and a batch environment are mainly in the mechanics of the program change. For example, the programmer may use cards to input the revised code in batch mode, or a terminal to enter the revisions online. The control objectives are the same, however, and the operating system considerations discussed in this chapter apply. Online library software is also available, and this chapter's discussion applies, as well, if management has implemented such software.

Minicomputers. Most of the minicomputers have user-oriented utility programs to provide the capabilities to perform many of the program change activities. Generally, few security features exist in these utility programs. Management may compensate for these missing features by exercising close supervision of computer operators, restricting the use of utility programs, and reviewing the output produced by the utility programs.

Service Centers. In a service center environment, some of the program change activities (that is, designing, programming, testing, and implementing changes) may be

performed by the service center rather than by client personnel. However, the responsibilities of these activities for control over program changes remain the same.

The auditor may be able to obtain information about the program change process and how the service center controls it from a third-party auditor's report or by visiting the service center.[4] The user should have compensating controls to provide reasonable assurance that the control objectives are met. For example, the user may wish to participate in the testing of program changes.

Conclusion

This section has offered some considerations regarding control over program changes. Achieving objectives of control over program changes should help prevent or detect errors or irregularities, such as these:

- Erroneous or invalid program changes.
- Lost or suppressed changes.
- Unauthorized changes.
- Improper reporting of program changes.
- Inadequate documentation of program changes.
- Implementation of insufficiently tested programs.

4. See *Audits of Service-Center-Produced Records* (New York: AICPA, 1974).

Case Study

The following case study is based on an actual system and has been included to show an example of the auditor's consideration of controls over using and changing computer programs. Although the auditor was concerned about many other audit-related areas, for illustrative purposes, this case is limited to the controls over using and changing the online savings systems programs.

ABC Savings and Loan Association is located in a regional metropolitan financial center and is in the $1 billion asset category. It provides online EDP capability to update either savings or loan accounts. Twenty-five branches are located in a one-hundred-mile radius of the home office. The association has a calendar year-end.

Audit Planning

In previous audits, the auditor had decided that reliance on the accounting procedures and controls performed by the computer programs was not possible because of poor control over program changes. The auditor had commented in the previous year's management letter on the lack of program change controls and had considered this weakness in planning the nature, timing, and extent of substantive testing. Otherwise, general controls had been satisfactory.

During this year's audit planning, the auditor decided that significant audit benefits could be derived if programmed controls in the savings system could be relied upon. The auditor noted that library software had been installed and new control procedures were to have been implemented. If relying on these controls were possible, the auditor would be able to reduce the extent of detailed transaction testing, confirmations, and testing of year-end balances. The auditor further determined that reliance on programmed controls would mean, in these circumstances, relying on controls over changes to computer programs.

To meet planned audit objectives, the auditor decided to obtain an updated description of the savings system and develop an understanding of the related flow of transactions and key accounting controls. This would be followed by an assessment of controls to determine if reliance appeared to be warranted. If so, the auditor would prepare a plan for performing compliance and substantive procedures. Because of the anticipated nature of compliance tests, the auditor planned to complete this phase of the audit by 7/31/XX.

Systems Description—Savings

In the preliminary phase of the study and evaluation of EDP accounting control, the auditor obtained a general understanding of the flow of transactions through the system. Customer transactions are entered six days per week through terminals located in the home office and branches. Tellers balance daily, and their reports are summarized in an office report by the head teller. Office reports are sent to the accounting department at the home office each night. Accounting department personnel balance office reports with transaction listings from the EDP department on the following business day.

Accounting department personnel coordinate correction of teller errors with head tellers who are responsible for appropriate error correction procedures. All non-teller-oriented transactions are initiated in the accounting department.

Teller keys are used for authorization of online savings, loan, and general transactions. Terminals are not restricted by function. Supervisor keys are available for control over

unusual transactions; for example, teller supervisors must insert a key in the terminal to permit activation of a dormant account. File maintenance and correction transactions are not initiated within EDP. All transaction activity is set forth in printed reports made available to the tellers and the accounting department. Management information reports are also available.

Authorization, execution, and recording of transactions using terminals are functions of both tellers and accounting department personnel. Accountability for recorded assets is the responsibility of the accounting manager. Accounting records are reviewed by the internal auditor, who reports monthly to the board of directors.

Savings System—Preliminary Evaluation

Based on the initial review of the savings system, the auditor concluded that programmed controls appeared to be used in the online savings system to (1) authorize transactions for processing, (2) provide documentation of the approved transactions and of rejected transactions, (3) process only programs activated by function keys on the terminal, and (4) update only valid and active savings accounts. The auditor also concluded that output reports appeared to be distributed to the proper people at the proper time and that the reports were reviewed and follow-up action was taken.

Based on the initial assessment, the auditor concluded that controls over the use of the online savings programs were sufficient to warrant design and implementation of compliance tests if the auditor could also rely on the controls over changes to programs. That is, to rely on the online savings controls, the auditor wanted assurance that the programs were the same throughout the year or were changed only in an authorized manner. Accordingly, the auditor decided to perform an initial review of the program change process to assess whether reliance on program change controls would be warranted.

System Description—Program Changes

The auditor noted that the EDP manager had installed program library software to manage the source program library. Other general controls noted in the previous year appeared to continue to be in effect. The client explained that the purpose of the library software was defined as "a control to assure that only authorized and correct versions of application production programs are processed." The client had installed this software based on a recommendation in last year's management letter. Documentation of the auditor's understanding of the new program change process is shown in the work papers in exhibits 1 and 2.

Program Changes—Preliminary Evaluation

Based on the initial review of the program change process, the auditor concluded that (1) users appeared to initiate documented change requests within their authority and to approve the changes before they are implemented; (2) systems and programming and an advisory committee approved changes in writing before implementation; and (3) systems programming personnel tested changes and updated documentation. The auditor, however, discovered that user personnel were not involved in nor did they review tests of the changes. Also, the person responsible for the librarian activity was in a position to conceal unauthorized program changes by not distributing library software update reports. This person was qualified as a programmer and had access to documentation, which could lead to a weakness in segregation of functions. There appeared to be no compensating controls for this weakness.

Audit Effects of Control Weaknesses

Because of these weaknesses, the auditor changed the planned approach to the audit of the savings system. As a result, the auditor decided not to pursue a detailed review of the program change process because it would not be appropriate to rely on it. Also, the auditor concluded that programmed controls identified in the savings system should not be relied upon because the extent of compliance testing would be too extensive to be justified economically and the usefulness of the results would be questionable. As a result, the auditor planned the scope of the current year's substantive procedures to be comparable to prior years.

EXHIBIT 1

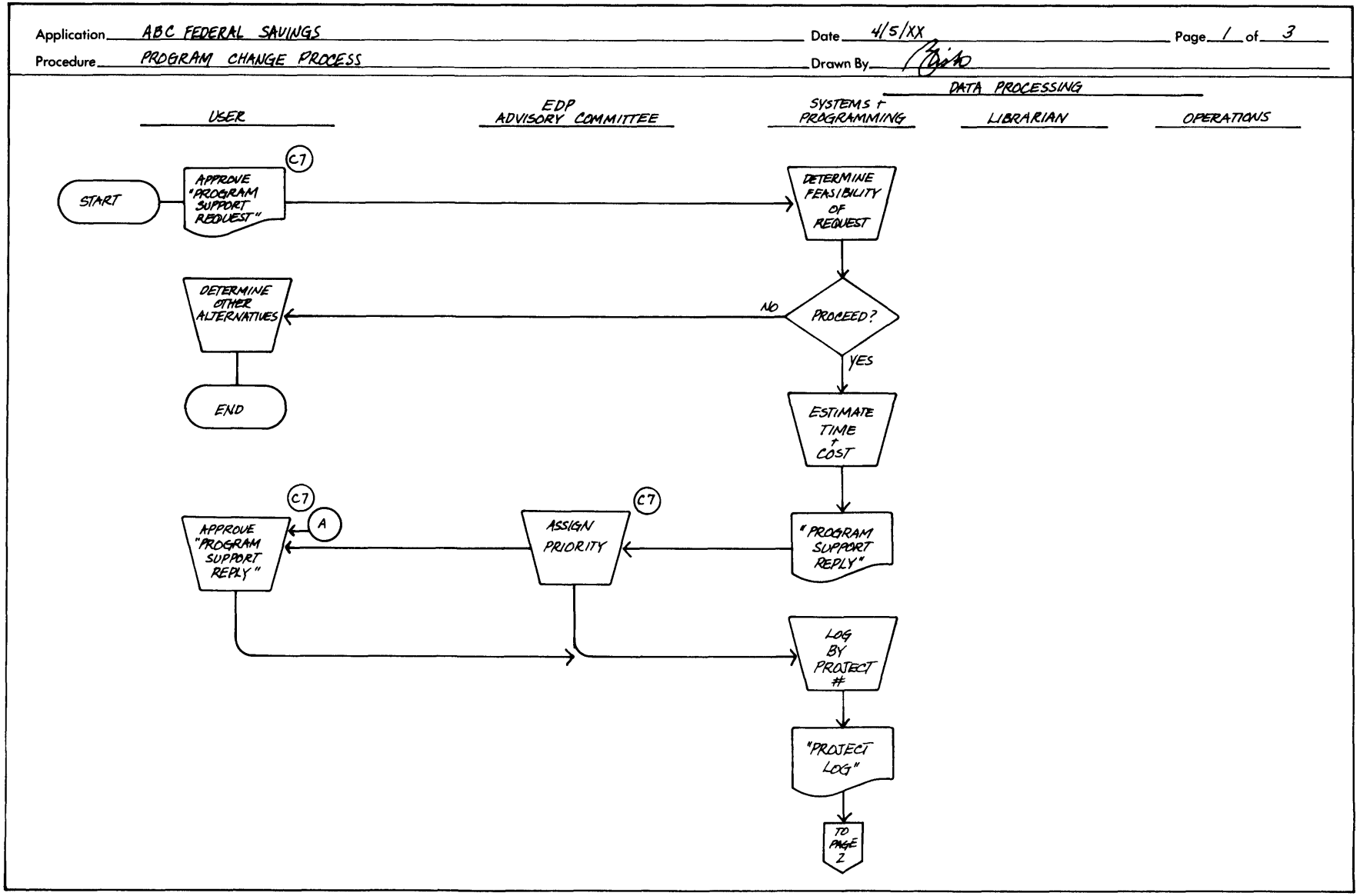

Application ABC FEDERAL SAVINGS
Date 4/5/XX
Page 1 of 3
Procedure PROGRAM CHANGE PROCESS
Drawn By
DATA PROCESSING
USER
EDP ADVISORY COMMITTEE
SYSTEMS & PROGRAMMING
LIBRARIAN
OPERATIONS
START
APPROVE "PROGRAM SUPPORT REQUEST"
C7
DETERMINE FEASIBILITY OF REQUEST
DETERMINE OTHER ALTERNATIVES
NO
PROCEED?
YES
END
ESTIMATE TIME & COST
C7
A
APPROVE "PROGRAM SUPPORT REPLY"
C7
ASSIGN PRIORITY
"PROGRAM SUPPORT REPLY"
LOG BY PROJECT #
"PROJECT LOG"
TO PAGE 2

EXHIBIT 1 (continued)

Application ABC - LIBRARY Date 4/5/XX Page 2 of 3

Procedure CHANGE PROCESS Drawn By

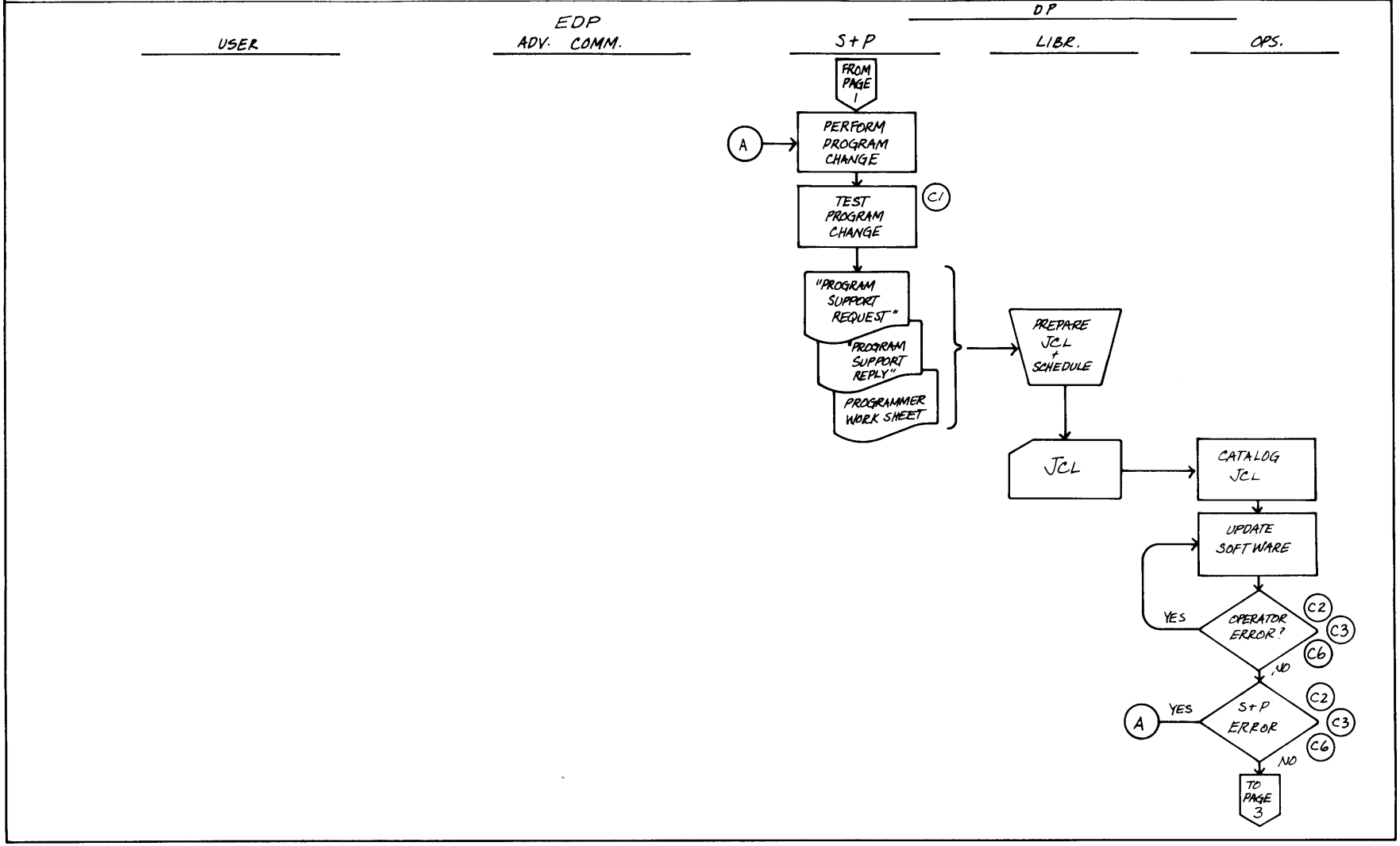


EXHIBIT 1 (continued)

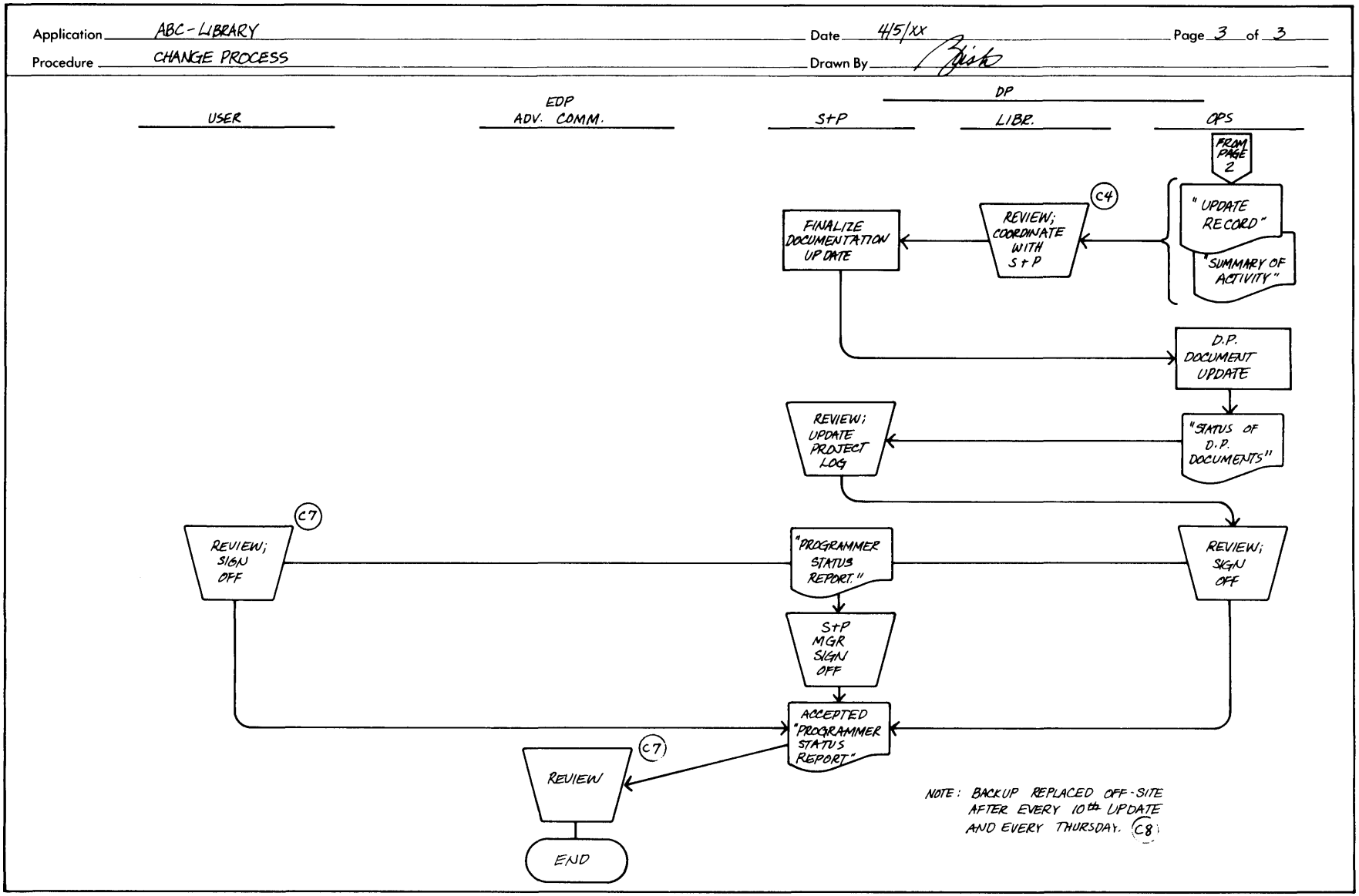


EXHIBIT 2

ABC FEDERAL SAVINGS —
PROGRAM LIBRARY SOFTWARE (1 OF 2)

TYPES OF ERRORS / IRREGULARITIES	PREVENTION / DETECTION TECHNIQUE	CONTROL (SEE FLOWCHART)
ERRONEOUS OR INVALID PROGRAM CHANGES	- SEGREGATION OF PRODUCTION AND TEST VERSIONS OF PROGRAMS	C1 - PACKAGE PROVIDES CAPABILITY FOR PROGRAMMER TO CREATE A SECOND VERSION OF A SOURCE PROGRAM UNDER A DIFFERENT NAME. THE SECOND VERSION MAY BE UPDATED WHILE PRODUCTION VERSION IS BACK UP COPY. POSSIBLE COMPLIANCE TEST: REVIEW PROCEDURES TO ASSURE THAT THE SECOND VERSION OF A PROGRAM IS CREATED ONLY FOR UPDATE PURPOSES
	- ERROR CORRECTION PROCEDURE	C2 - UPDATE ERRORS (SUCH AS INVALID SEQUENCE NUMBER) NOTED BY PACKAGE SUPPRESSES ALL CORRECTIONS AND OPTIONS. POSSIBLE COMPLIANCE TEST: REVIEW CORRECTION OF INVALID CARDS AND RESUBMISSION FOR PROPER UPDATE.
	- EDIT REPORT	C3 - PACKAGE COMPUTES A RANDOM FOUR CHARACTER CHECK DIGIT FOR EACH PROGRAM WHEN IT IS ADDED TO THE MASTER FILE. WHEN UPDATING OR DELETING, A PROGRAMMER MUST SUPPLY BOTH THE PROGRAM NAME AND THE CHECK DIGIT. IF ERRONEOUS, ALL ACTIVITY IS BYPASSED AND ERROR MESSAGE ISSUED. POSSIBLE COMPLIANCE TEST: TEST PROTECTION AGAINST UPDATING THE WRONG PROGRAM BY USING AN ERRONEOUS CHECK DIGIT.
	- TRANSACTION REPORT	C4 - "UPDATE RECORD" AND "SUMMARY OF ACTIVITY" LISTING IS PREPARED FOR REVIEW OF ALL PROGRAM CHANGES. THIS CONTROL IS LIMITED BECAUSE "SUMMARY" IS NOT RUN DAILY. POSSIBLE COMPLIANCE TEST: TEST LIBRARIAN REVIEW OF PRINTOUT REPORTS REFLECTING PROGRAM CHANGE ACTIVITY.

EXHIBIT 2 (continued)

ABC FEDERAL SAVINGS—
PROGRAM LIBRARY SOFTWARE (2 OF 2)

TYPES OF ERRORS / IRREGULARITIES	PREVENTION/DETECTION TECHNIQUE	CONTROL (SEE FLOWCHART)
LOST, SUPPRESSED, ADDED, DUPLICATED OR OTHERWISE IMPROPER PROGRAM CHANGES	-RESTRICTED ACCESS	C5 - LIBRARY PASSWORD ALLOWS MANAGEMENT TO PREVENT UNAUTHORIZED ACCESS TO RESTRICTED OR PRODUCTION PROGRAMS. THIS CONTROL IS LIMITED. PASSWORDS ARE GENERALLY AVAILABLE TO DP PERSONNEL. POSSIBLE COMPLIANCE TEST: TEST PASSWORD PROCEDURES
	-HASH TOTALS	C6 - PACKAGE COMPUTES A HASH TOTAL OF USER INPUT FOR EACH PROGRAM PROCESSED, STORING THE COUNT WITH THE PROGRAM. THIS PREVENTS AN UPDATE TO A MASTER WHICH HAD ALREADY BEEN UPDATED. POSSIBLE COMPLIANCE TEST: TEST ACCUMULATION OF HASH COUNT OF USERS INPUT AND REVIEW ERROR MESSAGES AND REJECTED TRANSACTIONS.
	-TRANSACTION REPORT	C4 - (ABOVE)
IMPROPER DISTRIBUTION OF OUTPUT	-USER REVIEW	C7 - USER AND EDP ADVISORY COMMITTEE REVIEWS "PROGRAMMER STATUS REPORT." POSSIBLE COMPLIANCE TEST: COMPARE TO INPUT REQUEST. EVALUATE EFFECTIVENESS OF REVIEWS.
LOSS OF OPERATIONS CONTINUITY	-BACKUP PROVISION	C8 - BACKUP REPLACED OFF-SITE AFTER EVERY TENTH UPDATE AND EVERY THURSDAY. POSSIBLE COMPLIANCE TEST: OBSERVE PROCEDURES AND EVALUATE EFFECTIVENESS.